THALES

Encryption and Authentication still Remain Base for Security in the AI Age

Marko Bobinac, PreSales Manager CEE

Thales © 2019 All rights reserved

Changes and product evolution are inevitable

The most powerful thing
about TIME is
It CHANGES

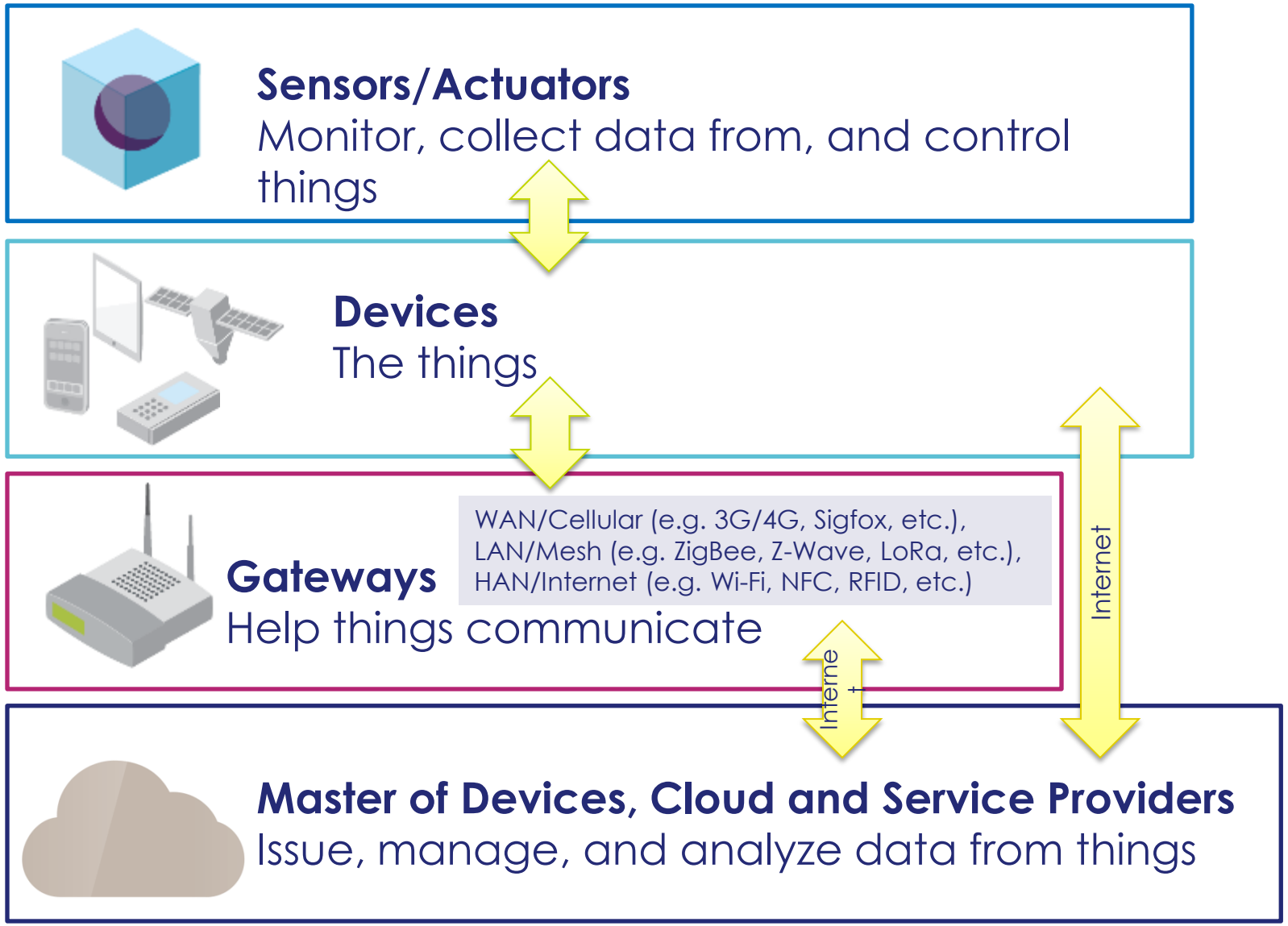
Thales © 2019 All rights reserved

New products, new technologies

Example No.1: something known and advanced

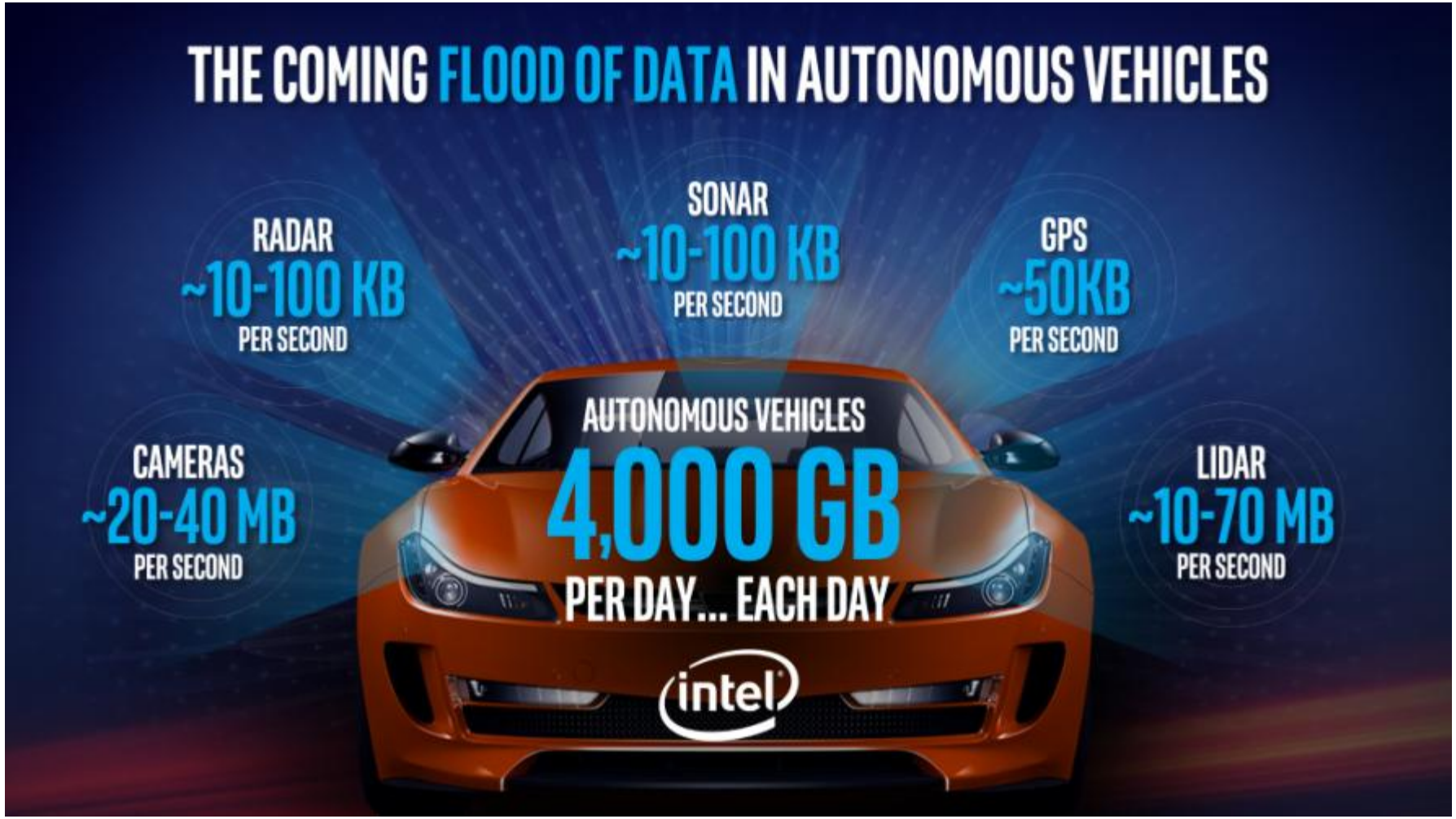
Thales © 2019 All rights reserved

Elements of the Internet of Things



Thales © 2019 All rights reserved

Data is the new oil



Masses of data need to be analyzed to be of value:
IoT helps to realize this value

Thales © 2019 All rights reserved

Automotive in driver's seat for IoT

82% of automotive leaders are confident
majority of cars will be connected by 2020 *(Vodafone)*

Thales © 2019 All rights reserved

Michelin Tires as a Service

Michelin have migrated from being a company that sells tires-as-a-product to a service that guarantees performance, which has led to:

- higher customer satisfaction,
- loyalty & retention and
- raised profits

Thales © 2019 All rights reserved

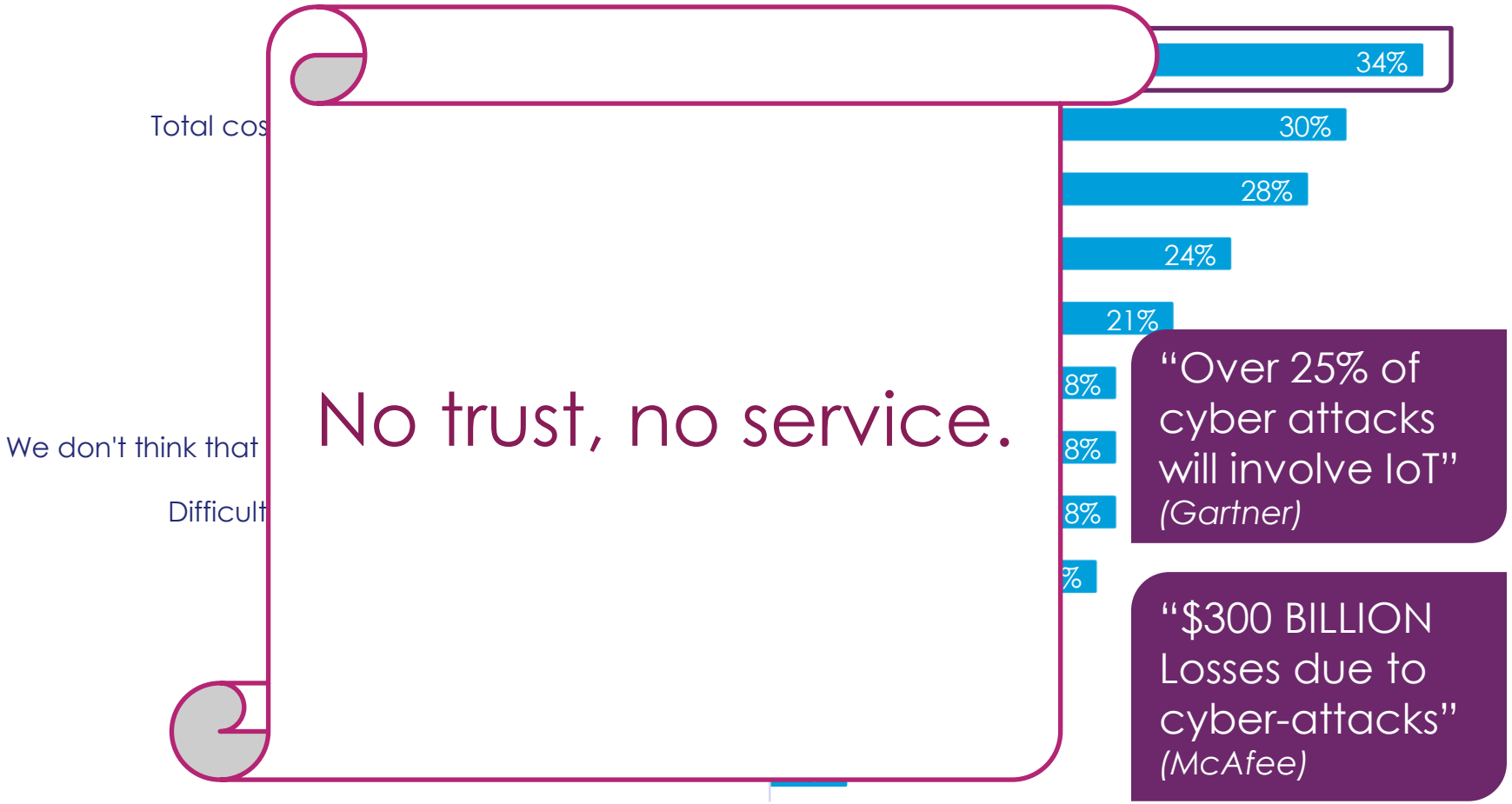
Kone IoT based Elevators & Escalators

Kone CEO "We are connecting elevators and escalators to the cloud – over 1 million by 2020.
With IoT and clould, we're collecting a lot of data, enabling us to reduce downtime"

Thales © 2019 All rights reserved

Security tops the list of IoT concerns

What are your firm's concerns, if any, with deploying M2M/Internet of Things technologies?

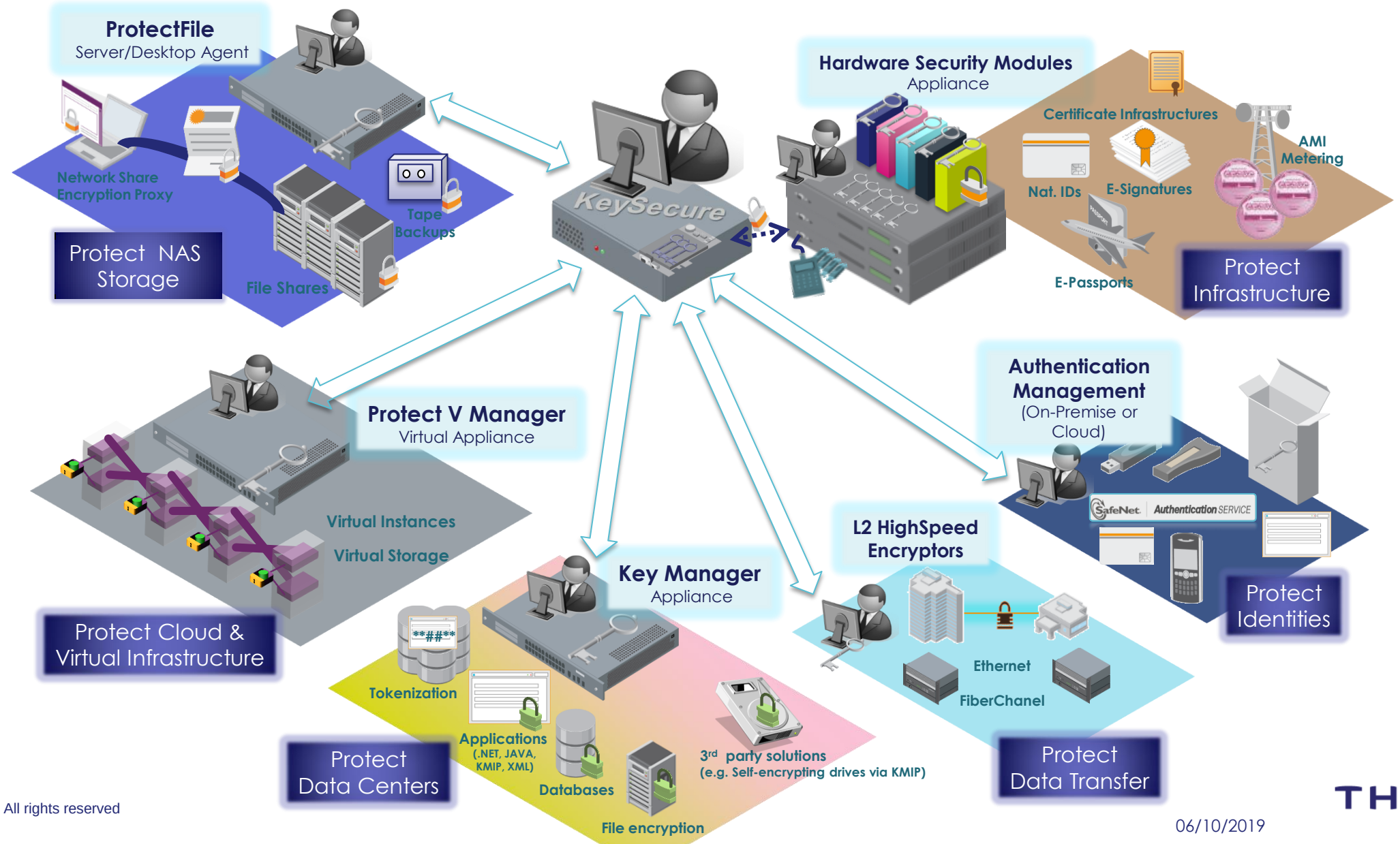


Base: 3627 global business and technology decision makers (20 + employees) in 7 online countries only

Source: Forrester's Global Business Technographics® Networks and Telecommunications Survey, 2015

Thales © 2019 All rights reserved

Thales provides foundation: Encryption and Authentication



Thales © 2019 All rights reserved

Customer Reality and Pain Point--Islands of Encryption

Database Encryption	Full Disk Encryption	Data Masking	Token-ization	Cloud Encryption	File Encryption	Access Policies	Secure File Sharing
Customer Records	Physical Security	PHI	PCI	Cloud Migration	Big Data	Privileged User Control	Storage Encryption

$ + $ + $ + $ + $ + $ + $ + $ + $ ...

Each use case requires individual infrastructure, management consoles and training

Complex • Inefficient • Expensive

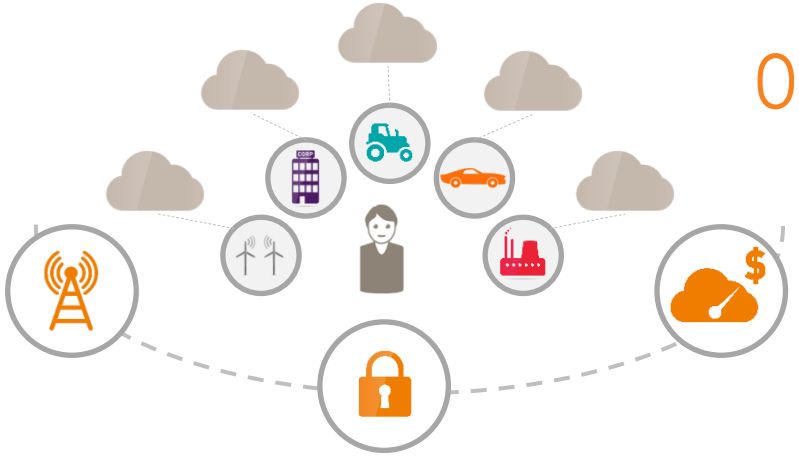
Thales © 2019 All rights reserved

THALES

Thales IoT Business Enablers

01 Connect

- Future-proof solutions
- Out-of-the-box connectivity
- Multiple form factors
- Quality of Service
- Subscription Management



03 Monetize

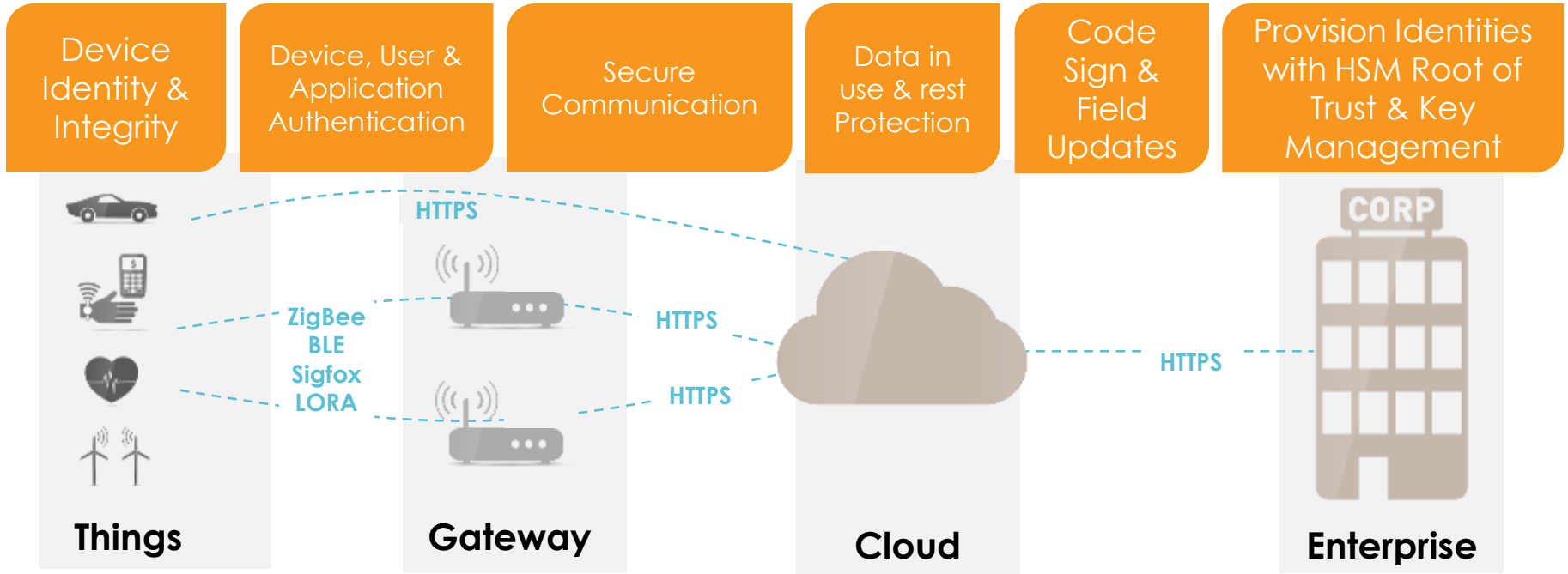
- Flexible revenue models
- Licensing and entitlement software
- IoT application development
- OTA upgrades

02 Secure

- Secure the device
- Secure the data
- Secure the cloud
- Secure the network
- Security Audit and lifecycle management

Thales © 2019 All rights reserved

Thales IoT security approach



Connect

Secure

Monetize

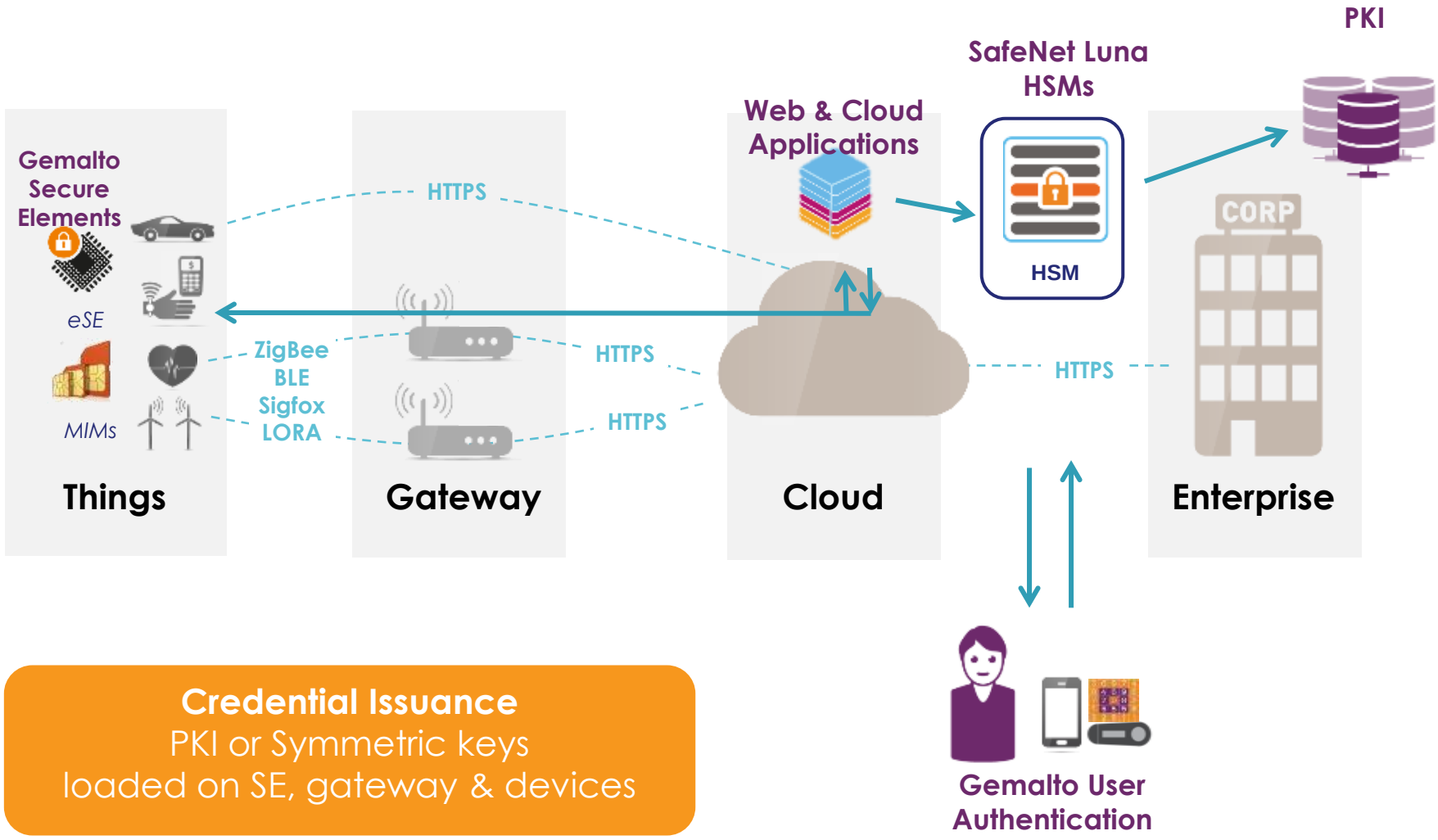
Thales Products

- Secure elements and embedded MIMs
- Machine to Machine modules and terminals
- Application enablement and delivery
- On-demand connectivity
- Trusted Service Hub & TKM Credential Provisioning
- Data encryption and device authentication
- Data encryption and user/application authentication
- Software Monetization: Feature based licensing & APIs for Enterprises

Thales © 2019 All rights reserved

THALES

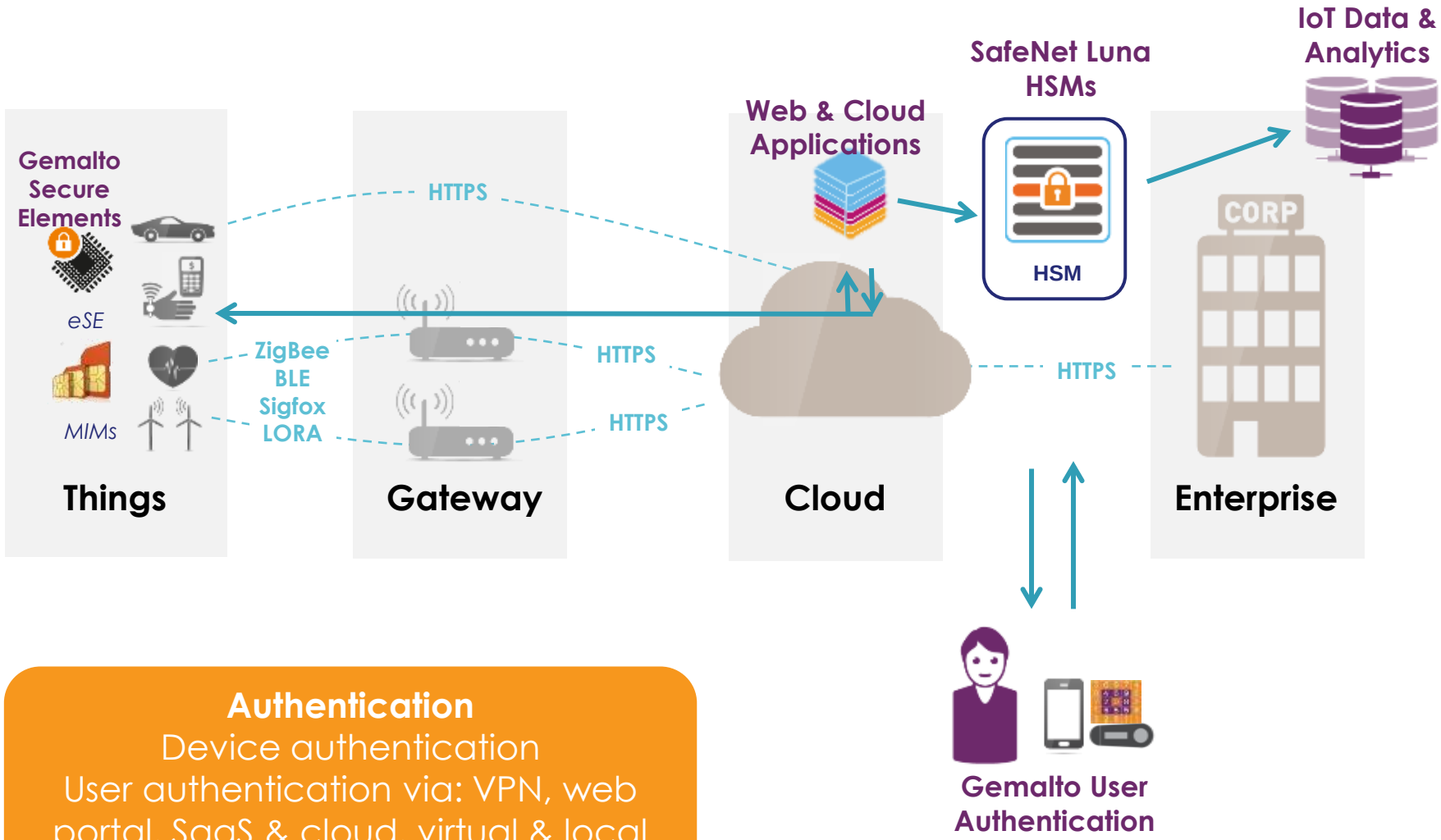
IoT security architecture:
Device, User & App Identity Issuance



Credential Issuance
PKI or Symmetric keys
loaded on SE, gateway & devices

Thales © 2019 All rights reserved
THALES

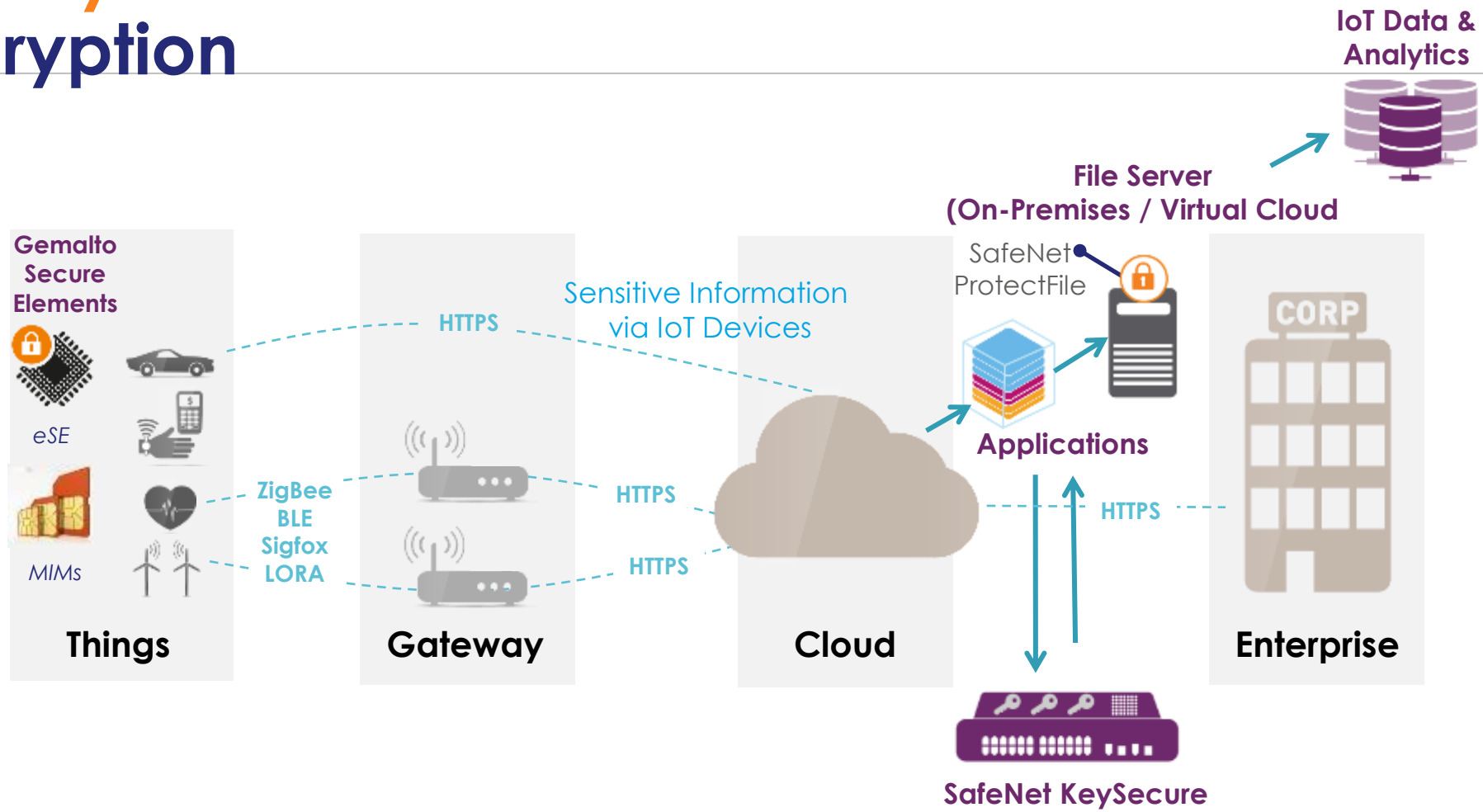
IoT security architecture:
Device, User & App Authentication



Authentication
Device authentication
User authentication via: VPN, web portal, SaaS & cloud, virtual & local networks

Thales © 2019 All rights reserved

IoT security architecture:
File encryption



CLOUD ENCRYPTION

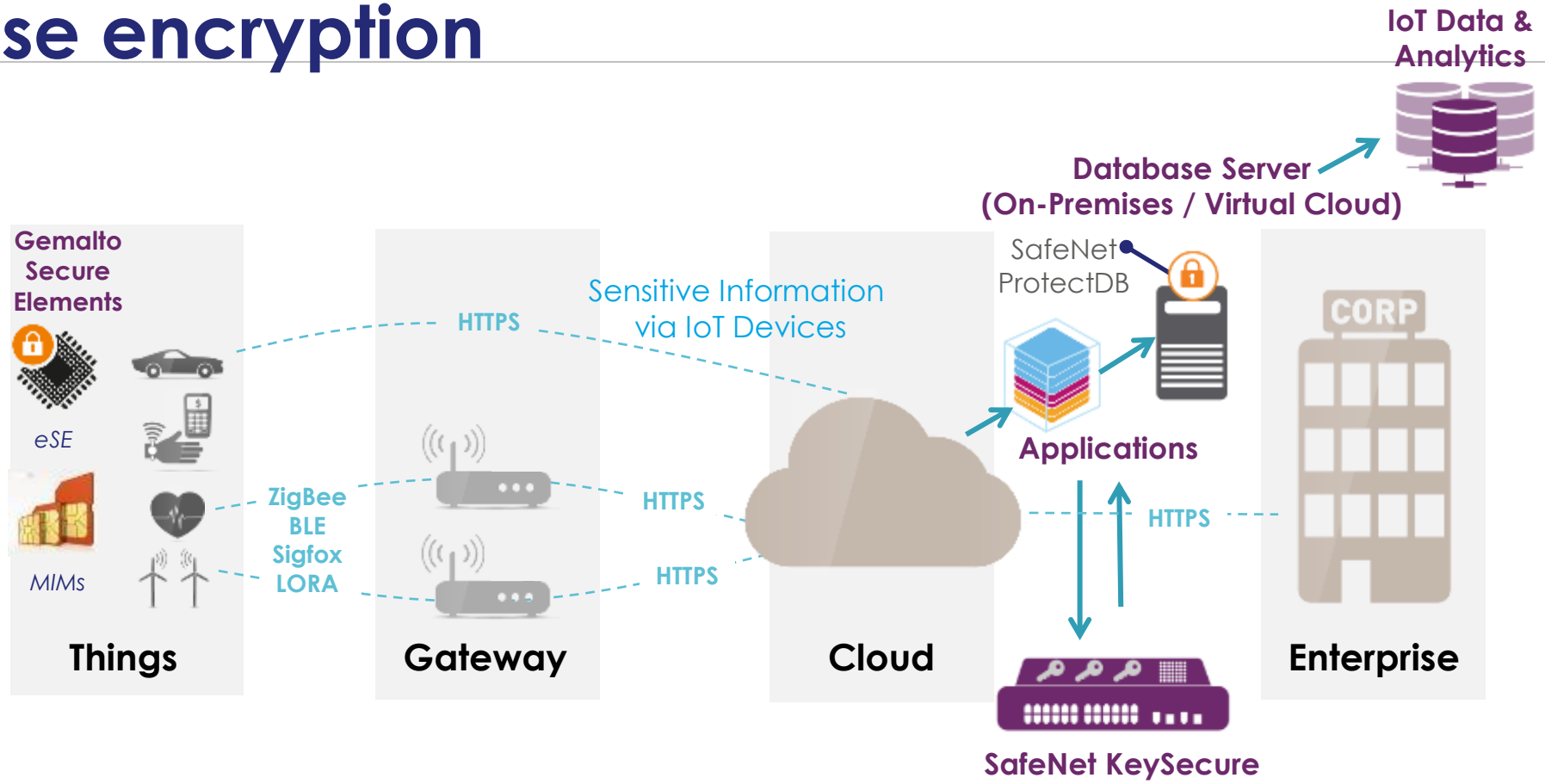
amazon web services
IBM SOFTLAYER
Google
vmware
Microsoft Azure

BIG DATA ENCRYPTION

hadoop
IBM InfoSphere BigInsights
Hortonworks
cloudera

Thales © 2019 All rights reserved
THALES

IoT security architecture:
Database encryption

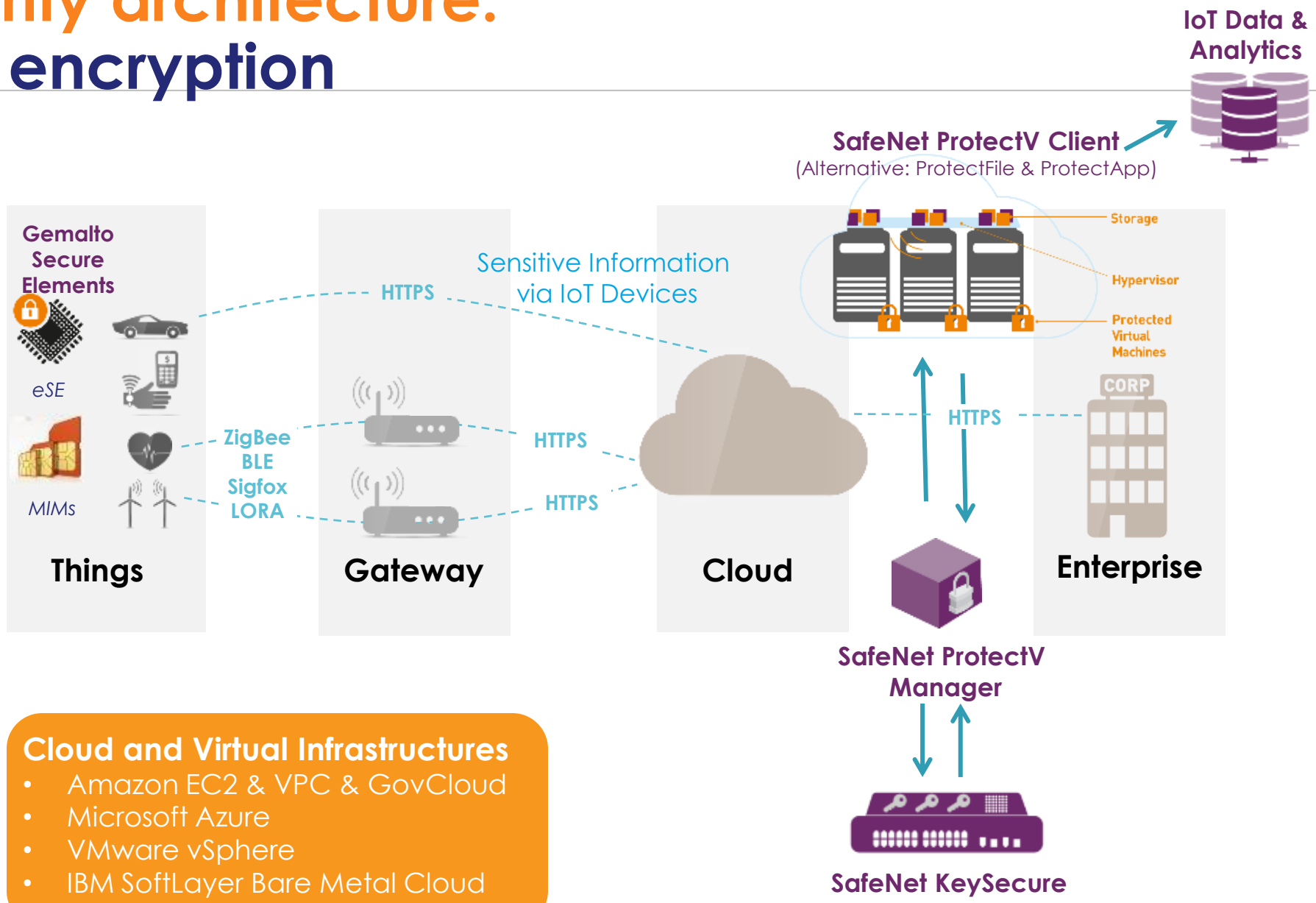


DATABASE ENCRYPTION

Couchbase · DATASTAX · mongoDB · Cassandra · ORACLE DATABASE · MariaDB · SAP · IBM DB2 · Microsoft SQL Server · SharePoint · MySQL · PostgreSQL

Thales © 2019 All rights reserved

IoT security architecture:
Volume encryption

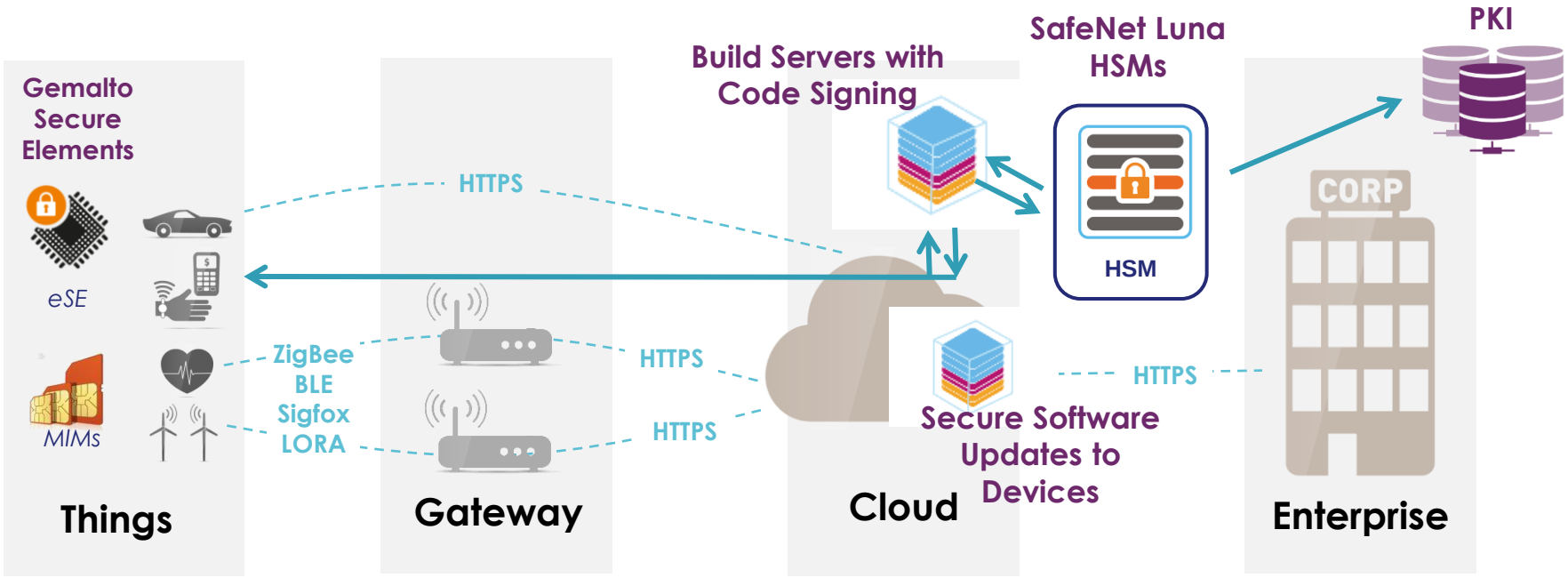


Cloud and Virtual Infrastructures

- Amazon EC2 & VPC & GovCloud
- Microsoft Azure
- VMware vSphere
- IBM SoftLayer Bare Metal Cloud

Thales © 2019 All rights reserved

IoT security architecture:
Code Signing & Software Updates

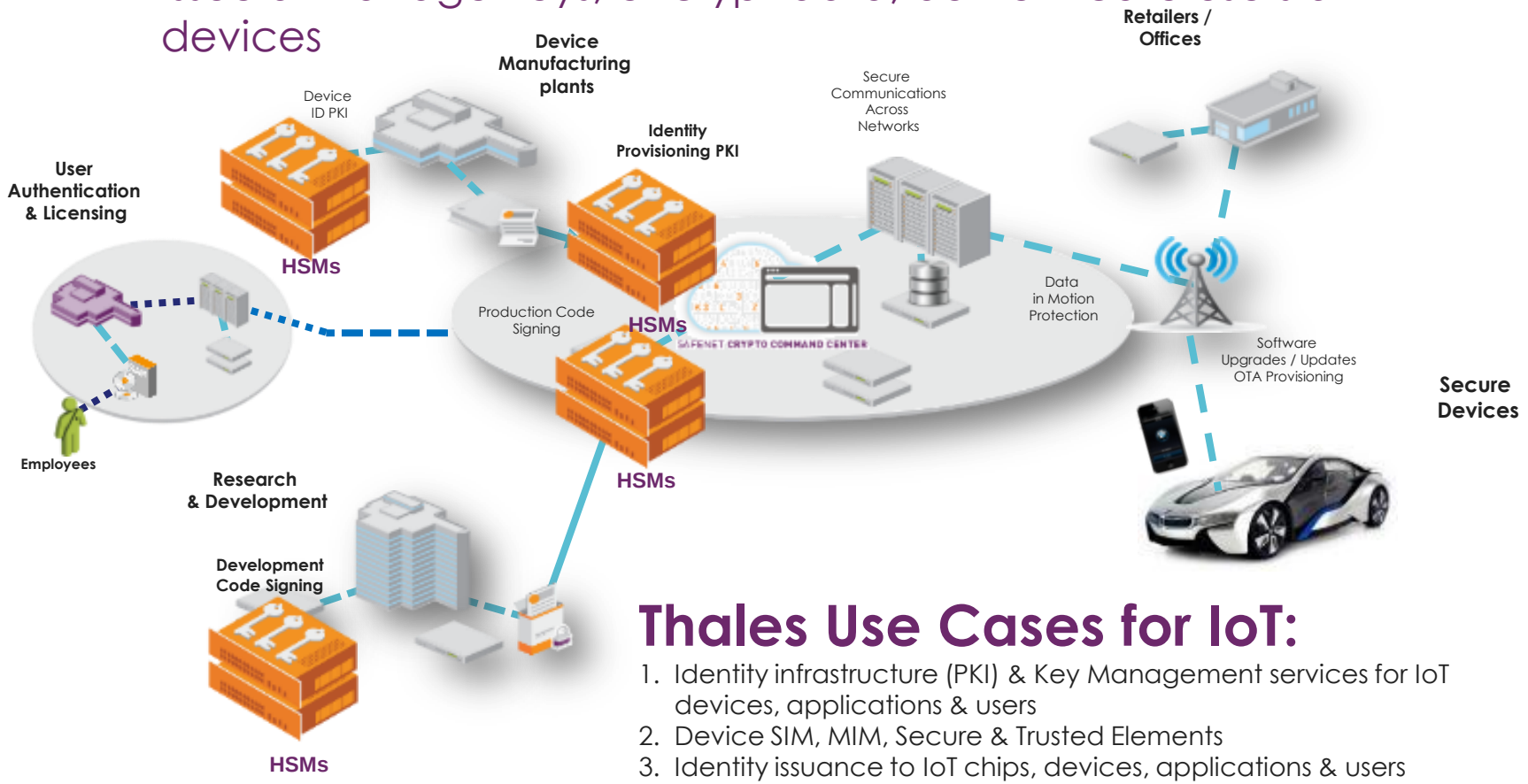


Code Signing
PKI or Symmetric keys to sign software loaded on SE, gateway & devices

Thales © 2019 All rights reserved

Thales provides Security foundation for IoT

Issue & manage keys, encrypt data, authenticate users & devices



Thales Use Cases for IoT:

1. Identity infrastructure (PKI) & Key Management services for IoT devices, applications & users
2. Device SIM, MIM, Secure & Trusted Elements
3. Identity issuance to IoT chips, devices, applications & users
4. Code signing Software/firmware/Updates for IoT devices
5. Authentication of IoT devices, users and applications
6. Secure Communications for IoT devices and applications (Data in motion)
7. Protection of IoT Data at rest for device, users, applications, Edge Compute & service providers
8. Protect data exchanges between IoT data centres (Data in motion)
9. Secure IoT payment transactions

Thales © 2019 All rights reserved

Example No.2: Artificial Inteligence

Deep fake ?

Thales © 2019 All rights reserved

AI Powered data manipulation

Deepfake (a portmanteau of "**deep** learning" and "**fake**") is a technique for human image synthesis based on **artificial** intelligence.

Xi Jinping

Justin Trudeau

Thales © 2019 All rights reserved

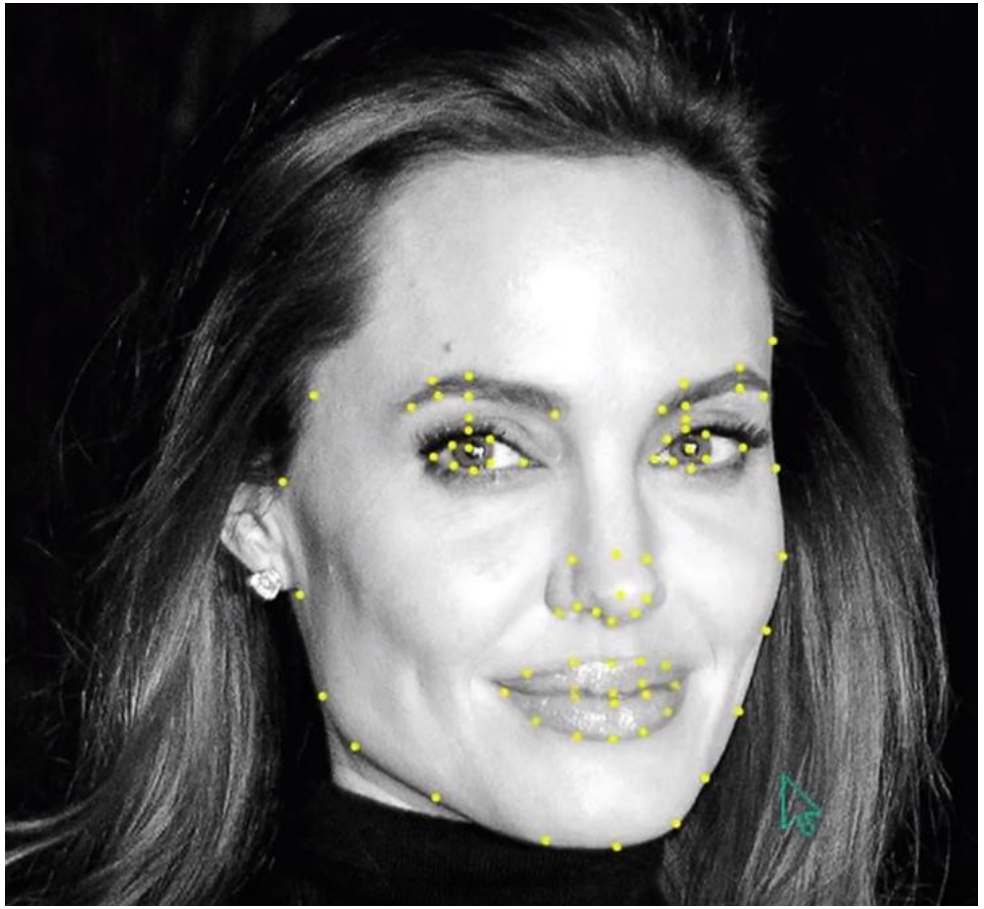
Deepfake process #1

- Feeding multiple audio, video or static samples into Neural network

Thales © 2019 All rights reserved

Deepfake process #2

- Neural network processes samples 1 by 1 and tries to learn specific characteristics



Thales © 2019 All rights reserved

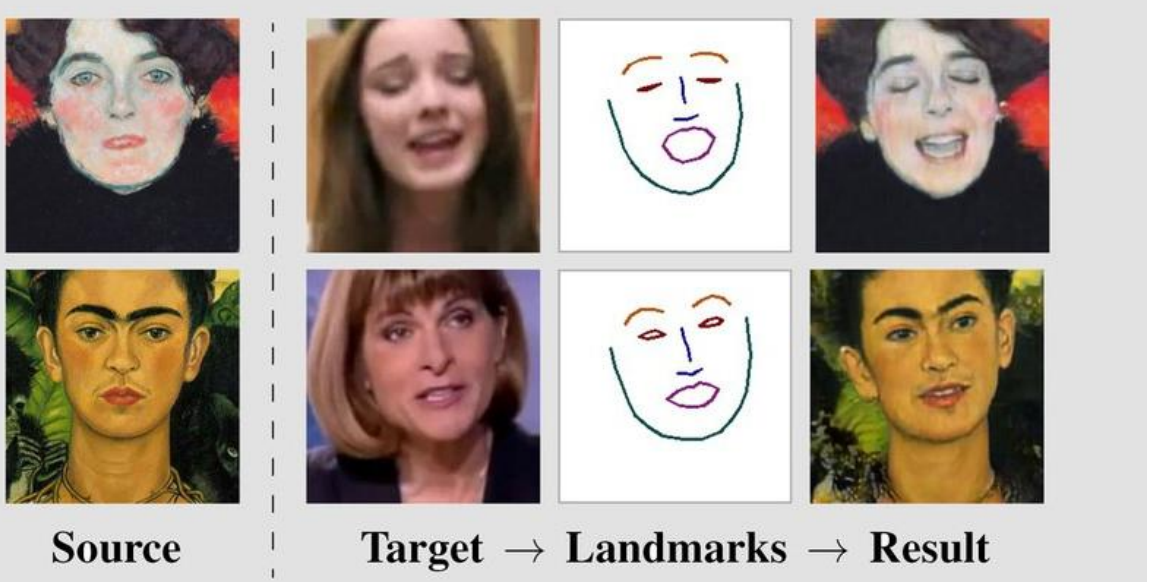
Deepfake process #3

Neural network models shape of mouth and other areas

Thales © 2019 All rights reserved

Deepfake process #4

Deep fake mimics Source „person“ by combining Target „person“ behaviour (characteristics)



Thales © 2019 All rights reserved

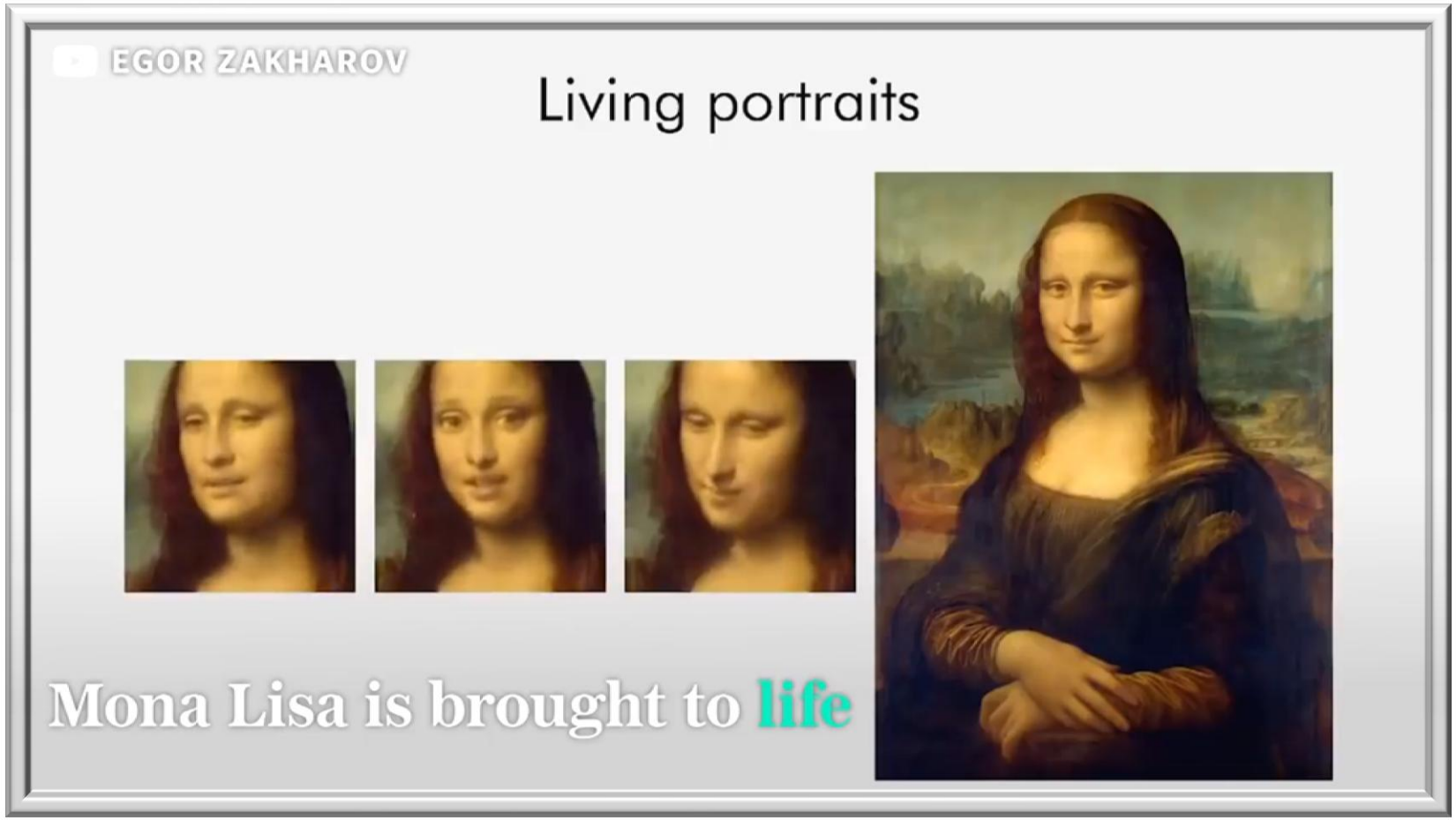
Deepfake example 1

Deep fake is capable of real-time processing by following speech and mimics of an impersonator

Thales © 2019 All rights reserved

Deepfake example 2

- More samples provide better results, but even single picture is enough



Thales © 2019 All rights reserved

Threat evolution

- Deep fake is visible and only one example of AI threat

- Artificial Intellience, Quantum computing and other technological advances break basic elements of Information Security theory: CIA model

Thales © 2019 All rights reserved

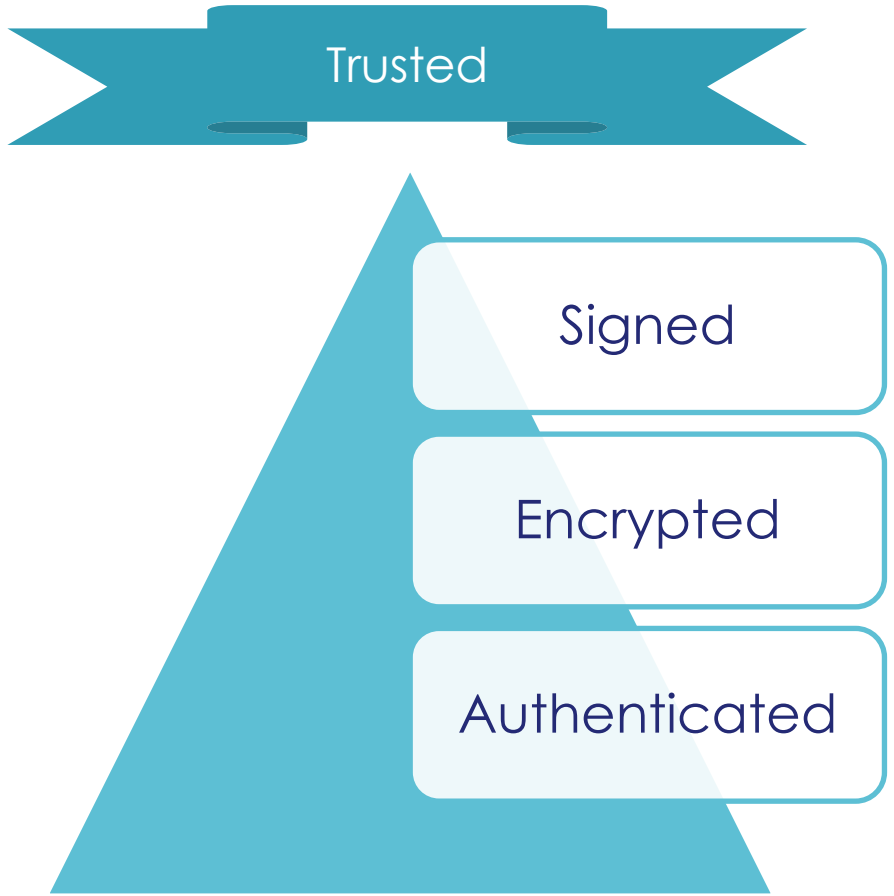
New threats, proven security technologies

~~So what we can do…~~

What we have to do…

Back to the basics of Information Security: Encryption and Authentication

- Signed videos and websites (SSL & media)
- Block-chaining video editing so it stays related to original source
- Encryption of data at rest to prevent stealing and manipulation
- User authetnication
  - Contributors
  - Content editors



Thales © 2019 All rights reserved

Thales CPL Comprehensive Data Security Products and Solutions

Protecting a world powered by the cloud, data and software

PKI

Create a Public Key Infrastructure to secure access to apps, protect your software from tampering, prevent unauthorized manufactured devices, and sign code & documents.

Big Data Security

Create isolation in your data lakes, mask sensitive data, and control admin users for security and compliance.

Data Security

Thales provides data security through encryption, key management, access control and security intelligence across devices, processes, platforms and environments.

Payment Security

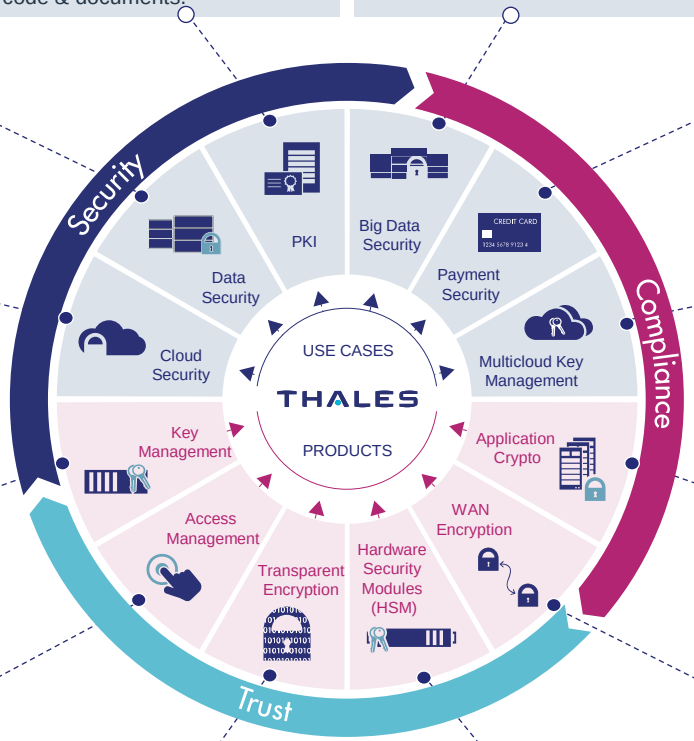
Enabling compliance, reduced risks, and increased operational efficiency for payment transactions across the globe.

Cloud Security

Secure your digital transformation with industry-leading encryption, key management, HSM and access management solutions from Thales.

Multicloud Key Management

Multicloud Lifecycle Key Management enables your team to efficiently control and report on BYOK and hybrid cloud key usage.



Key Management

The Vormetric Data Security Manager (DSM) provisions and manages keys for the Vormetric Data Security Platform and also manages keys and certificates for third-party devices

Application Crypto

Streamline secure development through APIs for tokenization, encryption and other cryptographic functions.

Access Management

Prevent breaches, move securely to the cloud and simplify compliance with Thales Access Management and Authentication solutions

WAN Encryption

Proven high-assurance network security for your sensitive data, real-time video and voice, on the move between data centers and sites.

Transparent Encryption

Encrypts, controls access to data and provides data access audit logging without impacting applications, databases or infrastructure – wherever servers are deployed.

Hardware Security Modules

A hardware security module (HSM) is a high-assurance crypto processor that provides a root of trust. Thales leads the industry in General Purpose, Payment and Cloud HSM solutions.

Thales © 2019 All rights reserved

THALES

Thales CPL: Unrivalled Data Protection Portfolio

The Market Leading Data Encryption Platforms

The Most Use Cases to Secure Data in the Cloud, Data Centers and Across Networks

SafeNet Luna Network HSM

payShield HSM

SafeNet Cloud HSM On Demand

Vormetric Data Security Platform

KeySecure

CipherTrust Cloud Key Manager

SafeNet High-Speed Network Encryptors

#1 General Purpose HSMs

#1 Payment HSMs

#1 Cloud HSMs

#1 Data Encryption

#1 Key Management

#1 Network Encryption

THALES

Conclusion

- **Hope is not a Strategy**

- **Start with the basics of Security foundation: Encryption and Authentication**
- Think about today‘s threats and prepare for tomorrow‘s AI and Quantum security challenges (Thales is already active in such protection)
- Choose the right partner for Today and Tomorrow.

Thales © 2019 All rights reserved

THALES

Thank you.

Thales © 2019 All rights reserved